

# Perancangan Kriptografi *Block Cipher* 256 Bit Berbasis pada Pola Tuangan Air

<sup>1</sup>Frellian Tuhumury, <sup>2</sup>Magdalena A. Ineke Pakereng, <sup>3</sup>Alz Danny Wowor

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Diponegoro 52-60, Salatiga 50711, Indonesia

Email: <sup>1</sup>672014714@student.uksw.edu, <sup>2</sup>ineke.pakereng@staff.uksw.edu,

<sup>3</sup>alzdanny.wowor@staff.uksw.edu

## **Abstract**

*Cryptography is the knowledge that used to secure the data. But cryptography needs to be updated or modified to improve the security. In this study, Block Cipher Cryptographic based at 256 Bit is designed with Cast Pattern Air, which has 20 rounds of the encryption process, and every process combined with the transformation using S-Box substitution table. Block Cipher 256 Bit cryptography based at Pattern Air produces a random encryption so that it can be used as an alternative in data security.*

**Keywords:** *Block Cipher, Cryptography, Cast Pattern Air*

## **Abstrak**

Kriptografi merupakan ilmu yang digunakan untuk mengamankan data. Tetapi kriptografi perlu di-*update* atau dimodifikasi untuk meningkatkan keamanan. Dalam penelitian ini dirancang Kriptografi *Block Cipher* 256 Bit Berbasis pada Pola Tuangan Air, yang memiliki 20 putaran proses enkripsi dan setiap proses dikombinasikan dengan transformasi menggunakan tabel substitusi *S-Box*. Kriptografi *Block Cipher* 256 Bit Berbasis Pola Tuangan Air memiliki hasil enkripsi yang acak sehingga dapat digunakan sebagai alternatif dalam pengamanan data.

**Kata Kunci:** *Block Cipher, Kriptografi, Pola Tuangan Air*

---

<sup>1</sup>Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

<sup>2</sup>Staf Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.Salatiga

<sup>2</sup>Staf Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.Salatiga

